(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2001 (13.09.2001)

PCT

(10) International Publication Number
WO 01/67667 A1

(51) International Patent Classification[7]: H04L 9/00, H04N 7/167

(21) International Application Number: PCT/US01/07206

(22) International Filing Date: 6 March 2001 (06.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
00200793.8 6 March 2000 (06.03.2000) EP
60/218,031 12 July 2000 (12.07.2000) US

(71) Applicants *(for all designated States except US)*: **ENTRIQ** [US/US]; 15070 Avenue of Science, Suite 200, San Diego, CA 92128 (US). **IRDETO ACCESS BV** [NL/NL]; Jupiterstraat 42, NL-2132 HD Hoofddorp (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WHITE, Mark, Andrew, George** [GB/US]; 6570 Ambrosia Lane, Apt. 1328, Carlsbad, CA 92009 (US). **WAJS, Andrew, Augustine** [GB/NL]; Schotersingel 93, NL-2023 AA Haarlem (NL).

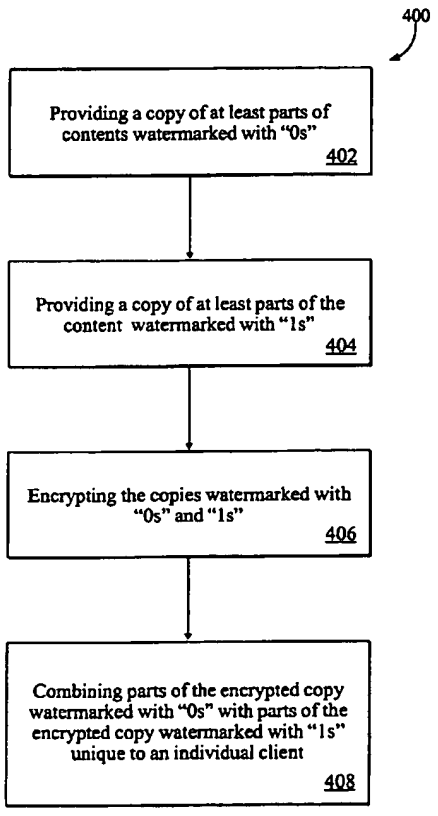
(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: METHOD AND SYSTEM TO UNIQUELY ASSOCIATE MULTICAST CONTENT WITH EACH OF MULTIPLE RECIPIENTS



(57) Abstract: Methods and systems are disclosed in which contact can be safely distributed and protected in a manner that is viable in terms of bandwidth economy and ensures that clients can be identified by the content (402) received. Copies of encrypted (406) content can be provided such that unique watermarks can be added to the copies. Content can also be both watermarked uniquely (408) for multiple clients and multicasted to the clients. As such, content can be distributed using the bandwidth efficiency of multicasting while providing reliable content protection and watermarking.

WO 01/67667 A1

patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *with international search report*

METHOD AND SYSTEM TO UNIQUELY ASSOCIATE MULTICAST CONTENT WITH EACH OF MULTIPLE RECIPIENTS

RELATED APPLICATIONS

[0001] This application is related to and claims priority to European Patent Application No. 00200793.8 entitled, "METHOD AND SYSTEM FOR PROVIDING COPIES OF SCRAMBLED CONTENT WITH UNIQUE WATERMARKS, AND SYSTEM FOR DESCRAMBLING SCRAMBLED CONTENT," filed on March 6, 2000, which is hereby incorporated herein by reference. This application is also related to and claims priority to U.S. Provisional Application No. 60/218,031 entitled, "METHOD AND SYSTEM TO UNIQUELY ASSOCIATE MULTICAST CONTENT WITH EACH OF MULTIPLE RECIPIENTS," filed on July 12, 2000, which is hereby incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention relates generally to data processing. More particularly, the present invention relates to "watermarking" or uniquely identifying content. Specifically, the present invention relates to a method and system to associate uniquely content with each of multiple recipients.

BACKGROUND OF THE INVENTION

[0003] Today, text, audio, and video content ("content") can be transmitted using a number of technologies. For example, a server on the Internet can transmit a video clip to a plurality of users. Such a process is typically referred to as "streaming." A number of challenges exist, however, for streaming content on the Internet. One challenge is content protection. The challenge of content protection relates to preventing illegal copying and distribution of premium content. Another challenge is bandwidth economics. The challenge of bandwidth economics relates to transmitting content within a limited bandwidth.

[0004] One method for content protection is watermarking. Watermarking is a process of inserting unique information ("watermark") into content in a non-removable manner. That is, an attempt to remove the watermark may cause loss of all or part of the

original content. A watermark is a form of rubber-stamping, e.g., a frame of a motion picture, with a unique signature. Typically, for a server on the Internet to perform watermarking, the server must send content with a different watermark for each user. Thus, a disadvantage of the watermarking process alone is that each item of content must be uniquely watermarked for each user or entity to whom the content is to be distributed. If the number of users to receive the content is large, watermarking can be bandwidth intensive and very complex for the server.

[0005] Another method for content protection is content encryption or scrambling. For example, in order to prevent unauthorized copying of content, the content can be encrypted with one or more keys and decrypted by users with correct keys to access the content. Generally, the content is both compressed and encrypted. A disadvantage of encrypting content alone is that after decrypting and descrambling the content unauthorized copies of the content can still be made. To locate the source of such unauthorized copying, a fingerprint or watermark can be added to content to indicate the content is copyright protected. A problem with adding a watermark to encrypted content is that it must be first decrypted before the watermark can be added. Consequently, if the content is encrypted, access to the content is not available. Moreover, adding watermarks and decrypting content requires extensive processing capacity.

[0006] One method to address bandwidth constraints is multicasting. Multicasting is the process of a single server sending content to multiple users at the same time. For example, a server on the Internet can send a video clip once ("multicast") to many users. Thus, a single server can send content to many users without either the server or the network becoming too congested. A disadvantage of multicasting alone is that it is difficult to protect the content being multicasted. For instance, multicasting is incompatible with existing watermarking technology because multicasting relies on all users receiving exactly the same data. Watermarking, however, relies on all users receiving uniquely "stamped" data. As such, a number of problems exist with distributing content such as text, audio, and video data on the Internet that relate to providing content within bandwidth constraints and ensuring content is protected or identified.

SUMMARY OF THE INVENTION

[0007] According to one aspect of the present invention, a method is disclosed in which a copy of at least one part of content having a first watermark is encrypted. A copy of at least one part of a content having a second watermark is encrypted. Parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark are combined in a manner unique for an individual client.

[0008] According to another aspect of the present invention, a method is disclosed in which first and second copies of content are watermarked with respective first and second watermarks. The first copy of the content is encrypted using a first key and the second copy of the content is encrypted using a second key. The encrypted first copy and second copy are combined into a single stream of data.

[0009] Other features and advantages of the present invention will be apparent from the accompanying drawings, and from the detailed description, which follows below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] The present invention is illustrated by way of example, and not limitation, by the figures of the accompanying drawings in which like references indicate similar elements and in which:

[0011] **FIG. 1** illustrates an exemplary diagram of a network environment in which the present invention can be implemented;

[0012] **FIG. 2** illustrates a diagram of encrypted content being combined according to one embodiment;

[0013] **FIG. 3** illustrates a block diagram of a content server communicating encrypted content with a client according to one embodiment;

[0014] **FIG. 4A** illustrates a flow chart of an operation to provide encrypted content according to one embodiment;

[0015] **FIG. 4B** illustrates a flow chart of an operation to decrypt encrypted content according to one embodiment;

[0016] **FIG. 5** illustrates a block diagram of a content server for unicasting keys and multicasting encrypted watermarked content according to one embodiment;

[0017] **FIG. 6A** illustrates a flow chart of an operation to create a single stream of data having encrypted content;

[0018] **FIG. 6B** illustrates a flow chart of an operation of distributing keys and the single stream of data of **FIG. 6A**;

[0019] **FIG. 7** illustrates exemplary video frames to perform the operation of **FIG. 6A**; and

[0020] **FIG. 8** is a block diagram of an exemplary digital processing or computing system in which the present invention can be implemented.

DETAILED DESCRIPTION

[0021] Methods and systems are described in which content can be safely distributed and protected in a manner that is viable in terms of bandwidth economy and ensures that clients can be identified by the content received. In one embodiment, copies of encrypted content can be provided such that unique watermarks can be added to the copies. In another embodiment, content can be both watermarked uniquely for multiple clients and multicasted to the clients. As such, content can be distributed using the bandwidth efficiency of multicasting while providing reliable content protection of watermarking.

[0022] In the following description, a watermark refers to an identifier or signature. For example, the identifier or signature can be used to indicate copyright protected data. The watermark can also be used to indicate the origin and authenticity of the data or the identity of clients/users/customers of the data. In addition, watermarking refers to a process of encrypting content in such a manner that it can be multicasted and still yield a unique version upon decryption. Furthermore, in the following description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be evident, however, to one skilled in the art that the present invention may be practiced without these specific details.

Exemplary Network Environment

[0023] **FIG. 1** illustrates an exemplary diagram of a network environment 100 in which the present invention can be implemented. Referring to **FIG. 1**, content server 104 can communicate with a plurality of clients 1 (101-1) through N (101-N) via network 102. In one embodiment, network 102 is the Internet. The Internet is a worldwide system of interconnected networks that runs the Internet Protocol (IP) to transfer data (e.g., packets). In other embodiments, network 102 can be other types of

networks such as, for example, a token ring network, local area network (LAN), or a wide area network (WAN). Network 102 can also be implemented in a wired or wireless environment.

[0024] Content server 104 is a network device for communicating on network 102. In one embodiment, content server 104 is a general purpose computer such as a web server. In other embodiments, content server 104 is a network device including a network router, switch, bridge, gateway, or other like network device, for communicating on network 102. Content server 104 includes a media server module 108 coupled to content storage 106. Content storage 106 is a storage device such as, for example, a hard disk, compact disk (CD), digital video disc (DVD), a random access memory (RAM), a dynamic random access memory (DRAM), or other like memory devices to store content for distribution.

[0025] In one embodiment, media server module 108 is a processing device to process instructions or code to perform the operations described herein. In other embodiments, media server module 108 is hardware and/or software modules to perform the same. Media server module 108 retrieves and processes content stored in content storage 106 and distributes the content to clients 1 through N. The content stored in content storage 106 can include video and/or audio data or other like types of data. For example, the content can include Moving Picture Experts Group (MPEG) data. In one embodiment, media server module 108 operates according to the processing techniques as described with respect to **FIGS. 2, 3, 4A** and **4B**. In another embodiment, media server module 108 operates according to the processing techniques as described with respect to **FIGS. 5, 6A, 6B**, and **7**.

[0026] Clients 1 through N can be general purpose computers for receiving content from content server 104 via network 102. Alternatively, clients 1 through N can be another content server such as content server 104. For example, clients 1 through N can be personal computers, workstations, laptop computers, or other like computing devices. Clients 1 through N can also be electronic portable devices such as, for example, a personal data assistant (PDA), wireless telephone, or other like devices, which can communicate with content server via network 102 over a wired or wireless medium. Clients 1 through N can include applications to view and display content from content

server 104. For example, clients 1 through N can include an application such as, for example, Real Player™ or QuickTime™ to play back video data.

Providing Copies of Encrypted Content with Unique Watermarks Example

[0027] The following embodiments with respect to **FIGS. 2, 3, 4A** and **4B** describe providing copies of encrypted content with unique watermarks for each of a plurality of clients and broadcasting the encrypted content to the clients. **FIG. 2** illustrates a diagram 200 of encrypted content being combined according to one embodiment. For purposes of explanation, the content is described as "movie content" but can easily be other types of content, e.g., an audio file of a record.

[0028] In one embodiment, content storage 106 includes three copies of movie content. Each copy stored in content storage 106 is encrypted in a suitable manner. A first copy 210 referred to as "neutral copy" is encrypted. A second copy 220 of the content is obtained by adding a watermark a first identifier, e.g., a sequence of "1s" or a more complex binary sequence, to at least one part of the complete content. Thereafter, second copy 220 is encrypted in a suitable manner so that an encrypted copy watermarked with the first identifier is obtained. A third copy 230 is obtained by adding a watermark with a second identifier, e.g., a sequence of "0s" or a more complex binary sequence, to at least one part of the complete content. Thereafter, third copy 230 is encrypted in a suitable manner so that an encrypted copy watermarked with the second identifier is obtained. Second and third copies 220 and 230 can be watermarked with any unique identifiers.

[0029] The watermarked copies 220 and 230 may include a percentage of the original movie content. For example, watermarked copies 220 and 230 may include 1% to 20% of the complete movie content. Nevertheless, the complete movie content can be watermarked with first and second identifiers, respectively. In an alternative embodiment, the neutral copy 210 can be omitted. Furthermore, copies 210, 220, and 230 can be stored on a separate storage device or on a separate server.

[0030] In one embodiment, if a client requests the movie content from content server 104, media module server 108 will add a watermark unique to the client. That is, in the example of **FIG. 2**, the watermark will be a unique identifier having unique sequences of ones ("1s") and zeroes ("0s"). In accordance with this unique sequence of ones and zeros, media module server 108 combines encrypted parts of the neutral copy 210, first

copy 220 watermarked with ones, and second copy 230 watermarked with zeroes and forwards the combination to the requesting client. As such, the requesting client receives an encrypted copy with watermarks unique to the client.

[0031] The watermarks, however, are not necessary to decrypt and encrypt the content in the relatively insecure environment of content server 104. The unique identification of ones and zeroes and associated client identification information can be stored in content storage 106 or in a separate storage device. Neutral copy 210 of scrambled content is used to reduce the amount of data that needs to be stored in content storage 106. Alternatively, a scrambled copy of content can be provided with a watermark without using neutral copy 210.

[0032] **FIG. 3** illustrates a block diagram 300 of content server 104 communicating scrambled content with a client 100 according to one embodiment. Client 100 can be representative of clients 1 through N in **FIG. 1**. Referring to **FIG. 3**, content server 104 includes media server module 108 having a receiving module 302 coupled to encryption module 304, which is coupled to key management module 306. Each of these modules can be a separate processing device or hardware and/or software modules operating within content server 104 to process instructions or code for performing the operations described herein.

[0033] Encryption module 304 encrypts content from receiving module 302. In one embodiment, receiving module 302 can receive content from content storage 106. In another embodiment, receiving module 302 receives content from network 102 or an external connection such as a cable or modem line. Encryption module 304 can encrypt content using keys in a standard encrypting process. For example, encryption module 204 can insert keys into a stream of video content as entitlement control messages (ECMs) to encrypt the stream of video content.

[0034] In one embodiment, watermarking can be performed on the client side. For example, client 100 can add watermarks during a decryption process for decrypting the encrypted content from content server 104. Client 100 can decrypt the encrypted content from content server 104 in real time or at a later time by storing the encrypted content.

[0035] In the following description for purposes of explanation, receiving module 302 in client 100 receives encrypted content that represents a "movie," which is to be broadcasted to client 100. Other types of content can be used such as text or audio

content that is commonly broadcasted. Receiving module 302 can be programmed to provide a plurality of double parts or so-called double illuminated parts for the movie. In one embodiment, if the movie is compressed, e.g., under the MPEG standard, I-frames or similar parts are double illuminated to keep bandwidth low. In one embodiment, receiving module 302 provides the double illuminated sections with a watermark. For example, receiving module 302 can add a watermark of zeros (or a first identifier) and a watermark of ones (or a second identifier) to selective sections of each double illuminated part. Receiving module 302 then forwards a neutral section and the double illuminated sections to encryption module 304.

[0036] Encryption module 304 uses keys provided by key management module 306. Key management module 306 can include one or more storage devices to store a number of keys to scramble content. In one embodiment, encryption module 304 uses a first key (Key 1) to encrypt the neutral section to provide neutral copy 210, a second key (Key 2) to encrypt watermarked sections with ones to provide second copy 220, and a third key to encrypt watermarked sections with zeros to provide third copy 230.

[0037] Key management module 306 in content server 104 includes a key management application to allow client 100 to receive a unique copy of encrypted content by delivering client keys 2 and 3 in a predetermined manner. Key management module 306 also allows client 100 to decrypt the encrypted content from encryption module 304. That is, key management module 100 provides the unique key information to client 100 via encryption module 304 to decrypt the encrypted content having a unique combination of encrypted sections watermarked with zeros (or first identifier) and sections watermarked with ones (or a second identifier). Furthermore, key management module 306 can store information related to which client received which unique combination. In this manner, client 100 can provide a clear content stream of the movie with a unique watermark or identification. Thus, the content stream can easily be identified to determine if the appropriate client is receiving and viewing the movie.

[0038] Key management module 306 can, for example, provide entitlement control messages ECMs with Key 1, Key 2, or Key 3. During broadcasting of the encrypted content, key management module 306 provides ECMs to respective clients containing the keys to obtain the unique combinations of ones and zeros at the respective clients. In

the example of **FIG. 3**, key management module 306 can provide the ECMs to client 100 via encryption module 304 or directly using an external connection to network 102.

[0039] Client 100 includes a receiving module 308 to receive encrypted content from content server 104. Receiving module 308 can also receive keys from key management module 306 within content server 104. Receiving module 308 is coupled to decrypting module 310, which is coupled to key management module 312. Each of these modules can be a separate processing device or hardware and/or software modules to process instructions or code for performing the operations described herein.

[0040] Client 100 uses decryption module 310 to decrypt the encrypted content from content server 104. Receiving module 308 receives encrypted content from encryption module 304 and extracts ECMs from the encrypted content and forwards the ECMs to key management module 312. Key management module 312 provides keys from the extracted ECMs to decryption module 310. Receiving module 308 also provides the encrypted content from content server 104 to decryption module 310.

[0041] In one embodiment, content server 104 provides ECMs with Key 1 and Key 2 or Key 3 unique to client 100. In particular, key management module 312 of client 100 delivers the keys to decryption module 310. Decryption module 310 uses the keys to obtain clear content with a unique combination of zeros and ones. In one embodiment, if only Key 2 is available, only the second watermark with ones can be decrypted whereas if only the third key is available only the section watermarked with ones can be decrypted. In this example, watermarking the neutral copy 210 is controlled directly by content server 104.

[0042] In an alternative embodiment, key management programs or instructions can be downloaded or permanently stored in key management module 312 within client 100. For example, key management module 312 can include a smart card to provide security to downloaded programs or instructions. In particular, the smart card could receive an ECM including all three keys (Key 1 through Key 3) in which the keys are provided to decryption module 310 in a manner unique to the smart card.

[0043] **FIG. 4A** illustrates a flow chart of an operation 400 to provide scrambled content according to one embodiment. Initially, operation 400 begins at operation 402.

[0044] At operation 402, a copy of at least parts of content watermarked with a first identifier (e.g., "0s") is provided. For example, receiving module 302 provides content watermarked with "0s" to encryption module.

[0045] At operation 404, a copy of at least parts of content watermarked with a second identifier (e.g., "1s") is provided. For example, receiving module 302 provides content watermarked with "1s" to encryption module.

[0046] At operation 406, the copies of the watermarked content with "0s" and "1s" is encrypted. In one embodiment, encryption module 304 can encrypt the watermarked content into three parts such as neutral copy 210 with a unique Key 1, a first copy 220 of encrypted content watermarked with "1s" with a unique Key 2, and a second copy 230 of encrypted content watermarked with "0s" with a unique Key 3.

[0047] At operation 408, parts of first copy 220 and second copy 230 are combined unique to an individual client. In one embodiment, parts of first copy 220 and second copy 230 are combined with neutral copy 210. In an alternative embodiment, parts of first copy 220 and second 230 are combined without neutral copy 210. Encryption module 304 can perform the above operation. Encryption module 304 or key management module 306 can send the unique keys (i.e., Keys 1 through 3) to a client to decrypt the content.

[0048] **FIG. 4B** illustrates a flow chart of an operation 450 to decrypt encrypted content according to one embodiment. Initially, operation 450 begins at operation 452.

[0049] At operation 452, unique keys are received, which are used by content server 104 to encrypt content. For example, receiving module 308 within client 100 can receive the unique keys. Receiving module 308 can forward the unique keys to key management module 312 or decryption 310 within client 100.

[0050] At operation 454, the encrypted content is received. The encrypted content is "double-illuminated" to refer that at least portions thereof are duplicated and watermarked with different identifiers. For example, client 100 can receive the encrypted content of operation 400 via receiving module 308. Encrypted content, however, can be received before the unique keys are received in operation 452.

[0051] At operation 456, the encrypted content is decrypted. For example, decryption module 310 can decrypt the encrypted content from content server 104 using the received unique keys.

Waterplexing Example

[0052] The following embodiments with respect to **FIGS. 5, 6A, 6B** and **7** describe a method and system to identify uniquely multicast content with each of multiple recipients. The following embodiments describe a "waterplexing" process by encrypting, e.g., a single data-stream of video content, in a manner that allows numerous unlocking keys to be distributed to a plurality of recipients ("customers"). Each key can decrypt the content into a unique form. In one embodiment, the content is encrypted once and then distributed to multiple clients. In order for the content to be unlocked and viewed, one or more unique keys are required to decrypt the content. That is, each unique key will cause the resulting decrypted content to be universally unique and viewable.

[0053] **FIG. 5** illustrates a block diagram 500 of content server 104 for unicasting keys and multicasting encrypted content according to one embodiment. Referring to **FIG. 5**, content server 104 includes content storage 106 for storing content, which is coupled to server media module 108. In one embodiment, server media module 108 includes a watermarking module 506 coupled to content storage 106 and encryption module 507, which is coupled to keys database 508. Each of these modules can be a separate processing device or hardware and/or software modules to process instructions or code for performing the operations described herein.

[0054] Content storage 106 stores content that is to be multicasted. For example, content storage 106 can store text, audio, and video content. In the following embodiments, content storage 106 stores a stream of video data. Watermarking module 506 processes the stream of video data in content storage 106. In one embodiment, watermarking module 506 adds unique watermarks or stamps to redundant data (e.g., frames or packets within the stream of video data) for a waterplexing process. That is, redundant pieces (e.g., "frames") of data are included in the stream of video data. The watermarks or stamps refer to any modification to one or more frames of video that result in detectable information being added to those frames. Watermarking module 506 forwards the watermarked frames to encrypting module 507.

[0055] Encrypting module 507 encrypts the watermarked frames. In one embodiment, because some frames are repeated in the video stream, encrypting module 507 can uniquely encrypt each frame of repeated frames. As such, unique encryption and decryption keys can be used and associated with each redundant frame. Keys

database 508 can store such keys. Keys database 508 can include one or more tables of keys, which are mapped for unique clients/users/customers ("customers"), which will be described below. In one embodiment, encrypting module 507 unicasts unique keys from keys database 508 for individual customers. Encrypting module 507 can also multicast watermarked content, which has been encrypted, to all the customers requesting to receive the multicast. In an alternative embodiment, encrypting module 507 can multicast first and then unicast the keys.

[0056] **FIG. 6A** illustrates a flow chart of an operation 600 to create a single stream of data having encrypted video frames. Initially, operation 600 begins at operation 602.

[0057] At operation 602, selected frames within the stream of video data stored in content storage 106 are watermarked. For example, as shown in **FIG. 7**, frames 715 represents original content of 5 frames. Watermarking module 506 can provide unique watermarks to the repeated frames. The amount of repetition that occurs is not relevant except that repetition does occur, which allows for part of the whole to be uniquely encrypted. In the example of **FIG. 7**, visible letters are stamped onto the bottom right of the repeated frames as shown in frames 725.

[0058] At operation 604, the selected watermarked frames and remaining frames are encrypted with unique keys. As shown in frames 735 of **FIG. 7**, the stamped frames are encrypted using unique keys that follow the uniqueness of the stamps. That is, if the stamp is unique then the key is unique. The remaining frames are encrypted using a common key. For example, the frames stamped with "ADA," "LME," "XRD," and "QEW" are encrypted with unique keys. The non-stamped or watermarked frames are encrypted with the common key.

[0059] At operation 606, the frames 735 are combined into a single data stream as shown in frames 745 of **FIG. 7**. The single stream of data, i.e., frames 745 can be multicasted to requesting customers. In one embodiment, the common key is sent to all customers. The combination of the other keys set to a customer dictates which frames can be decrypted and thus which stamps will be in the customer's decrypted version. In one embodiment, the decryption keys unique to each customer are unicasted to the customer.

[0060] Since frames can be repeated and uniquely stamped and uniquely encrypted, a two-dimensional array of key/stamp pairs can be constructed for any given item of

content. The array has a width equal to the number of times a frame is selected for unique stamping, and has a depth equal to the number of times a frame is repeated.

[0061] As shown in **FIG. 7**, individual frames in frames 725 were selected for watermarking of stamping. Here, two watermarks or stamps are used thus requiring an array with a width of two. Within each stamping selection, each frame is repeated twice, which requires a depth of 2. As shown in **Table 1** below, a 2x2 array is shown mapping unique keys to individual stamps.

Table 1

Frames 2 & 3	Frame 5
Key1 = ADA	Key3 = LME
Key2 = XRD	Key4 = QEW

[0062] By choosing which keys to send to any given customer, it can be determined as to which stamps will be present in the content once decrypted. For example, the above array has four potential combinations. Thus, four uniquely identifiable versions could exist after decryption. An exemplary **Table 2** is shown below associating individual customers with which keys are to be received based on the stamps in the content.

Table 2

Consumer	Keys received	Stamps in content
Michael	Key 1, Key 3	ADA, LME
Donald	Key 2, Key 4	XRD, QEW
Jane	Key 1, Key 4	ADA, QEW
Mary	Key 2, Key 3	XRD, LME

[0063] With repetition of parts of a video-stream, video content can be encrypted in a manner that guarantees uniqueness of the decrypted version. This concept relies on the fact that no customer is given all of the keys required for an item of content, but is given a unique combination of keys just sufficient to decrypt the content to a viewable state.

[0064] Most popular video compression techniques involve using key frames (or I frames) to begin a sequence of animation, which is then followed by data that describes how the remaining frames sequentially differ from each other. In one embodiment, since

the waterplexing example described above relies on repetition of video frames, a waterplexing engine can be used in conjunction with a video compression engine to determine where key-frames occur in order to provide a compression solution.

[0065] **FIG. 6B** illustrates a flow chart of an operation 650 of distributing keys and the single stream of data of **FIG. 6A**. Initially, operation 650 begins at operation 652.

[0066] At operation 652, the unique keys are unicasted. For example, the keys in **Tables 1** and **2** above are unicasted to one or more clients or customers.

[0067] At operation 654, the single data stream having unique watermarks and encrypted with unique keys is multicasted. For example, the frames 745 shown in **FIG. 7** are multicasted to one or more clients or customers. In other embodiments, the order of operation 652 and operation 654 can be reversed.

[0068] Thus, the above operations described in **FIGS. 6A** and **6B** show how to uniquely associate multicast content with each of multiple clients or customers.

Exemplary Digital Processing or Computing System

[0069] FIG. 8 is a block diagram of an exemplary digital processing system 800 for a content server or a client. For example, digital processing system 800 can represent content server 104 as described in FIGS. 1, 2, and 5. Digital processing system 800 may store a set of instructions for causing the system to perform any of the operations as explained above. Digital processing system 800 can also represent a client on a network or other types of network devices, which include a network router, a network switch, or a network bridge or gateway. Digital processing system 800 can also represent a client being a portable electronic device such as, for example, a personal data assistant, a mobile device, a web appliance, or any other type of machine capable of executing a sequence of instructions that specify actions to be taken by that machine.

[0070] Referring to FIG. 8, digital processing system 800 includes a bus 808 coupled to a central processing unit (CPU) 802, main memory 804, static memory 806, network interface 822, video display 810, alpha-numeric input device 812, cursor control device 814, drive unit 816, and signal generation device 820. The devices coupled to bus 808 can use bus 808 to communicate information or data to each other. Furthermore, the devices of digital processing system 800 are exemplary in which one or more devices can be omitted or added. For example, one or more memory devices can be used for digital processing system 800.

[0071] The CPU 802 can process instructions 826 or instructions 826 stored in main memory 804 or a machine-readable medium 824 within drive unit 816 via bus 808. For one embodiment, CPU 802 can process and execute instructions 826 to implement the operations as described in FIGS. 2A, 2B, 6A, and 6B. Bus 808 is a communication medium for communicating data or information for digital processing system 800.

[0072] Main memory 804 can be, e.g., a random access memory (RAM) or some other dynamic storage device. Main memory 804 stores instructions 826, which can be used by CPU 802. Main memory 804 may also store temporary variables or other intermediate information during execution of instructions by CPU 802. Static memory 806, can be, e.g., a read only memory (ROM) and/or other static storage devices, for storing information or instructions, which can also be used by CPU 802. Drive unit 816 can be, e.g., a hard or floppy disk drive unit or optical disk drive unit, having a machine-readable medium 824 storing instructions 826. The machine-readable medium 824 can also store other types of information or data.

[0073] Video display 810 can be, e.g., a cathode ray tube (CRT) or liquid crystal display (LCD). Video display device 810 displays information or graphics to a user. Alpha-numeric input device 812 is an input device (e.g., a keyboard) for communicating information and command selections to digital processing system 800. Cursor control device 814 can be, e.g., a mouse, a trackball, or cursor direction keys, for controlling movement of an object on video display 810. Signal generation device 820 can be, e.g., a speaker or a microphone.

[0074] Digital processing system 800 can be connected to a network 102 via a network interface device 822. Network interface 822 can connect to a network such as, for example, a local area network (LAN), wide area network (WAN), token ring network, Internet, or other like networks. Network interface device 822 can also support varying network protocols such as, for example, hypertext transfer protocol (HTTP), asynchronous transfer mode (ATM), fiber distributed data interface (FDDI), frame relay, or other like protocols.

[0075] Thus, a method and system to uniquely identify multicast content with each of multiple recipients have been described. In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto

without departing from broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative sense rather than a restrictive sense.

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:

encrypting a copy of at least one part of content having a first watermark;

encrypting a copy of at least one part of the content having a second watermark; and

combining parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

2. The computer-implemented method of claim 1, wherein the first watermark includes "0s" and the second watermark includes "1s."

3. The computer-implemented method of claim 1, further comprising:

distributing the combined parts to one or more clients on a network.

4. The computer-implemented method of claim 3, wherein the network includes an Internet network.

5. The computer-implemented method of claim 1, further comprising:

encrypting a neutral part of the content; and

combining parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

6. A server comprising:

a storage device to store content; and

an encryption module to encrypt a copy of at least one part of the content having a first watermark, to encrypt a copy of at least one part of the content having a second watermark, and to combine parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

7. The server of claim 6, wherein the first watermark includes "0s" and the second watermark includes "1s."

8. The server of claim 6, wherein the server is to distribute the combined parts to one or more clients on a network.

9. The server of claim 6, wherein the network includes an Internet network.

10. The server of claim 6, wherein the encryption module is to encrypt a neutral part of the content and to combine parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

11. A computing system comprising:

means for storing content; and

means for encrypting a copy of at least one part of the content having a first watermark, a copy of at least one part of the content having a second watermark; and

means for combining parts of the encrypted copy with the first watermark and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

12. The computing system of claim 11, wherein the first watermark includes "0s" and the second watermark includes "1s."

13. The computing system of claim 11, further comprising:

means for distributing the combined parts to one or more clients on a network.

14. The computing system of claim 13, wherein the network includes an Internet network.

15. The computing system of claim 11, further comprising:

means for scrambling a neutral part of the content; and

means for combining parts of encrypted neutral copy, parts of the encrypted copy with the first watermark, and parts of the encrypted copy with the second watermark in a manner unique for an individual client.

16. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:

encrypting a copy of at least one part of content having a first watermark;

encrypting a copy of at least one part of the content having a second watermark; and

combining parts of the scrambled copy with the first watermark and parts of the scrambled copy with the second watermark in a manner unique for an individual client.

17. A digital processing system comprising:

a storage device to store an encrypted copy of at least one part of content watermarked with a first identifier and an encrypted copy of at least one part of the content watermarked with a second identifier; and

a processing unit coupled to the storage device, the processing unit to combine parts of the encrypted copy watermarked with the first and second identifiers unique to an individual client.

18. The digital processing system of claim 17, wherein the processing unit is to send the combined parts to the individual client.

19. The digital processing system of claim 17, wherein the first identifier includes "0s" and the second identifier includes "1s."

20. The digital processing system of claim 17, wherein the storage device is to store a client identification and a corresponding unique combination of watermarked copies for the client.

21. The digital processing system of claim 17, wherein the storage device is to store a neutral scrambled copy of the content.

22. The digital processing system of claim 21, wherein the processing unit is to combine at least one part of the neutral encrypted copy with parts of the encrypted copy watermarked with the first identifier and with parts of the encrypted copy watermarked with the second identifier.

23. A digital processing system comprising:

a receiving module to provide clear content having a plurality of double parts, a first part watermarked with a first identifier and a second part watermarked with a second identifier;

an encryption module coupled to the receiving module, the encryption module to encrypt the clear content with a first key, to encrypt the first part watermarked with the first identifier with a second key, and to encrypt the second part watermarked with the second identifier with a third key; and

a key management module to manage the keys as to allow one or more clients to decrypt the encrypted content with a combination of encrypted first and second parts watermarked with the first identifier and second identifier, respectively, unique to each client.

24. The digital processing system of claim 23, wherein the first identifier includes "0s" and the second identifier includes "1s."

25. The digital processing system of claim 23, wherein the encryption module is to provide entitlement control messages (ECMs) using the first key, second key, and third key, wherein the second and third key are alternated to obtain a unique combinations of "0s" and "1s" unique to each client.

26. The digital processing system of claim 23, wherein the storage device is to store a client identification and a corresponding unique combination of watermarked copies for the client.

27. A computer-implemented method comprising:

watermarking first and second copies of content with respective first and second watermarks;

encrypting the first copy of content using a first and the second copy of the content using a second key; and

combining encrypted copies into a single stream of data.

28. The computer-implemented method of claim 27, further comprising:

multicasting the single stream of data to one or more clients.

29. The computer-implemented method of claim 27, further comprising:

storing the unique keys and common key in a database, the database including an array matching the unique keys to the unique watermarks.

30. The computer-implemented method of claim 29, further comprising:

selectively unicasting the unique keys to one or more clients.

31. The computer-implemented method of claim 30, further comprising:

associating each client to the unique keys received and watermarks in the stream of data.

32. A server comprising:

a storage device to store content;

a processing unit to watermark redundant parts in the content with one or more unique watermarks, to encrypt the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key, and to combine the encrypted parts into a single stream of data.

33. The server of claim 32, wherein the processing unit is to multicast the single stream of data to one or more clients.

34. The server of claim 32, further comprising:

a database to store the unique keys and common key, the database including an array matching the unique keys to the unique watermarks.

35. The server of claim 32, wherein the processing unit is to unicast selectively the unique keys to one or more clients.

36. The server of claim 32, wherein the processing unit is to associate each client to the unique keys and watermarks in the stream of data.

37. A computing system comprising:

means for storing content;

means for watermarking redundant parts in the content with one or more unique watermarks;

means for encrypting the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key; and

means for combining the encrypted parts into a single stream of data.

38. The computing system of claim 37, further comprising:

means for multicasting the single stream of data to one or more clients.

39. The computing system of claim 37, further comprising:

means for storing in a database the unique keys and common key, the database including an array matching the unique keys to the unique watermarks.

40. The computing system of claim 37, further comprising:

means for unicasting selectively the unique keys to one or more clients.

41. The computing system of claim 37, further comprising:

means for associating each client to the unique keys and watermarks in the stream of data.

42. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:

watermarking redundant parts in content with one or more unique watermarks;

encrypting the watermarked redundant parts using a unique key for each unique watermark and the remaining parts of the stream of content with a common key; and

combining encrypted parts into a single stream of data.

43. A method of distributing content, the method comprising:

watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying both the first and second duplicates of the content portion to first and second users; and

supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

44. The method of claim 43, wherein the content includes text, audio, or video content.

45. The method of claim 43, wherein the supplying of the first and second duplicates and keys includes supplying the first and second duplicates and keys via a network.

46. The method of claim 45, wherein the network includes an Internet network.

47. An apparatus comprising:

watermarking means for watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting means for encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying means for supplying both the first and second duplicates of the content portion to first and second users; and

supplying means for supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

48. The apparatus of claim 47, wherein the content includes text, audio, or video content.

49. The apparatus of claim 47, wherein the supplying means for the first and second duplicates and keys include supplying means for supplying the first and second duplicates and keys via a network.

50. The apparatus of claim 49, wherein the network includes an Internet network.

51. A machine-readable medium providing instructions, which if executed by a processor, causes the processor to perform an operation comprising:

watermarking first and second duplicates of a content portion with first and second identifiers respectively;

encrypting each of the first and second duplicates of the content portion with at least first and second keys respectively;

supplying both the first and second duplicates of the content portion to first and second users; and

supplying at least the first key to the first user and the second key to the second user, so that the first user is enabled to decrypt the first duplicate of the content portion watermarked with the first identifier, and so that the second user is enabled to decrypt the second duplicate of the content portion watermarked with the second identifier.

52. A method of distributing content, the method comprising:

watermarking multiple sets of duplicated content portions with multiple sets of identifiers, each identifier of each set being unique to a specific duplicated content portion;

encrypting each duplicated content portion within each set with a respective key of a plurality of keys;

supplying the multiple sets of duplicated content portions to multiple users; and

supplying a unique set of keys, selected from the plurality of keys, to each of the multiple users so that each of the multiple users is enabled to decrypt the multiple sets of duplicated content portions to generate content embodying a unique sequence of identifiers.

53. The method of claim 52, wherein the supplying of the multiple sets of duplicated content portions includes multicasting the multiple sets of duplicated content portions to the multiple users on an Internet network.

54. The method of claim 53, wherein the supplying of the unique sets of keys to each of the multiple users includes unicasting the unique set of keys to each of the multiple users on the Internet network.

55. The method of claim 52, wherein the content portions include text, audio, or video content portions.

56. An apparatus comprising:

watermarking means for watermarking multiple sets of duplicated content portions with multiple sets of identifiers, each identifier of each set being unique to a specific duplicated content portion;

encrypting means for encrypting each duplicated content portion within each set with a respective key of a plurality of keys;

supplying means for supplying the multiple sets of duplicated content portions to multiple users; and

supplying means for supplying a unique set of keys, selected from the plurality of keys, to each of the multiple users so that each of the multiple users is enabled to decrypt the multiple sets of duplicated content portions to generate content embodying a unique sequence of identifiers.

57. The apparatus of claim 56, wherein the supplying means for supplying of the multiple sets of duplicated content portions includes multicasting means for multicasting the multiple sets of duplicated content portions to the multiple users on an Internet network.

58. The apparatus of claim 57, wherein the supplying means for supplying of the unique sets of keys to each of the multiple users includes unicasting means for unicasting the unique set of keys to each of the multiple users on the Internet network.

59. The apparatus of claim 56, wherein the content portions include text, audio, or video content portions.

60. A machine-readable medium providing instructions, which if executed by a processors, causes the processor to perform an operation comprising:

watermarking multiple sets of duplicated content portions with multiple sets of identifiers, each identifier of each set being unique to a specific duplicated content portion;

encrypting each duplicated content portion within each set with a respective key of a plurality of keys;

supplying the multiple sets of duplicated content portions to multiple users; and

supplying a unique set of keys, selected from the plurality of keys, to each of the multiple users so that each of the multiple users is enabled to decrypt the multiple sets of duplicated content portions to generate content embodying a unique sequence of identifiers.

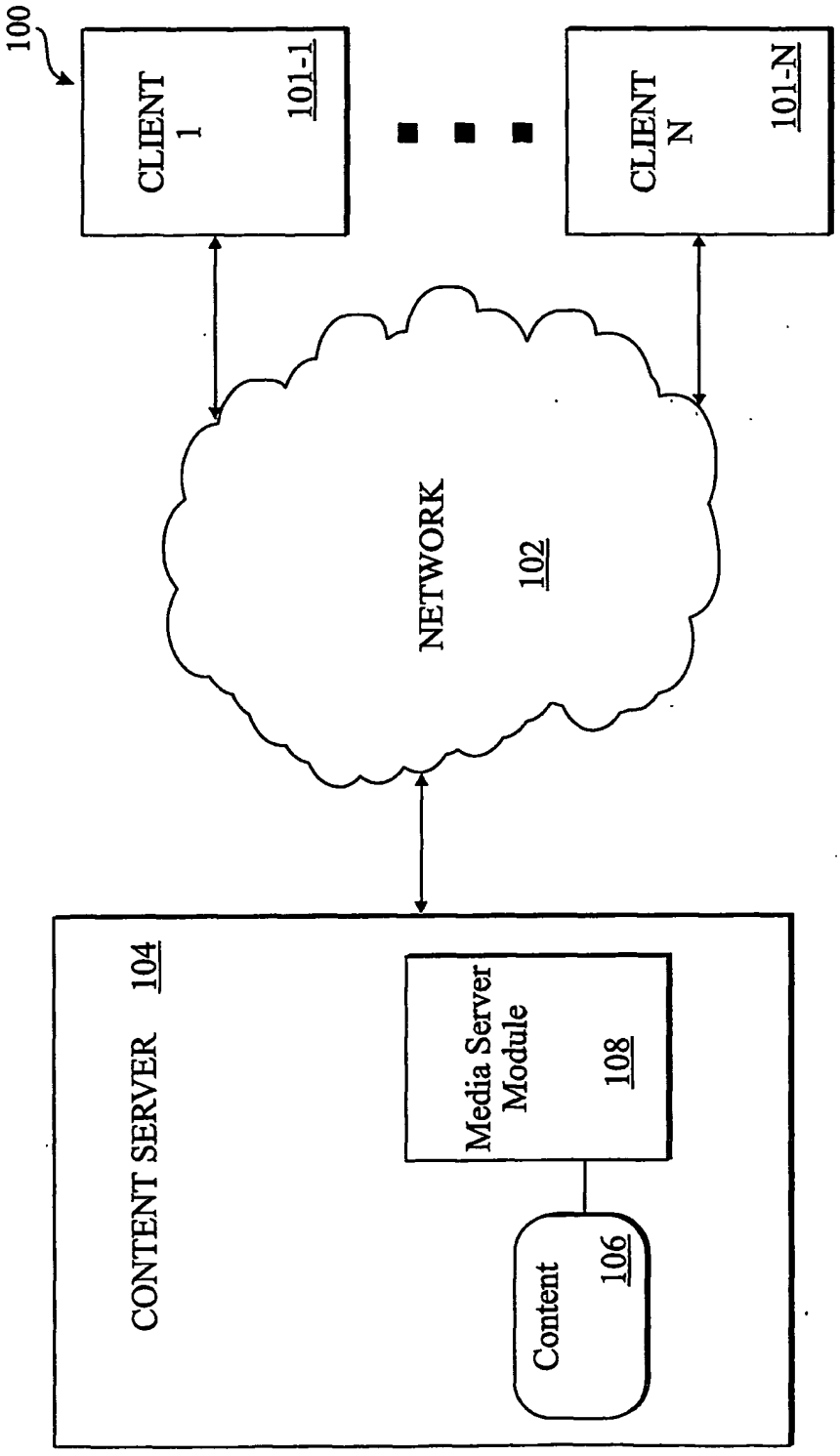

100
CLIENT 1
101-1
CLIENT N
101-N
NETWORK
102
CONTENT SERVER
104
Media Server Module
108
Content
106

Fig. 1

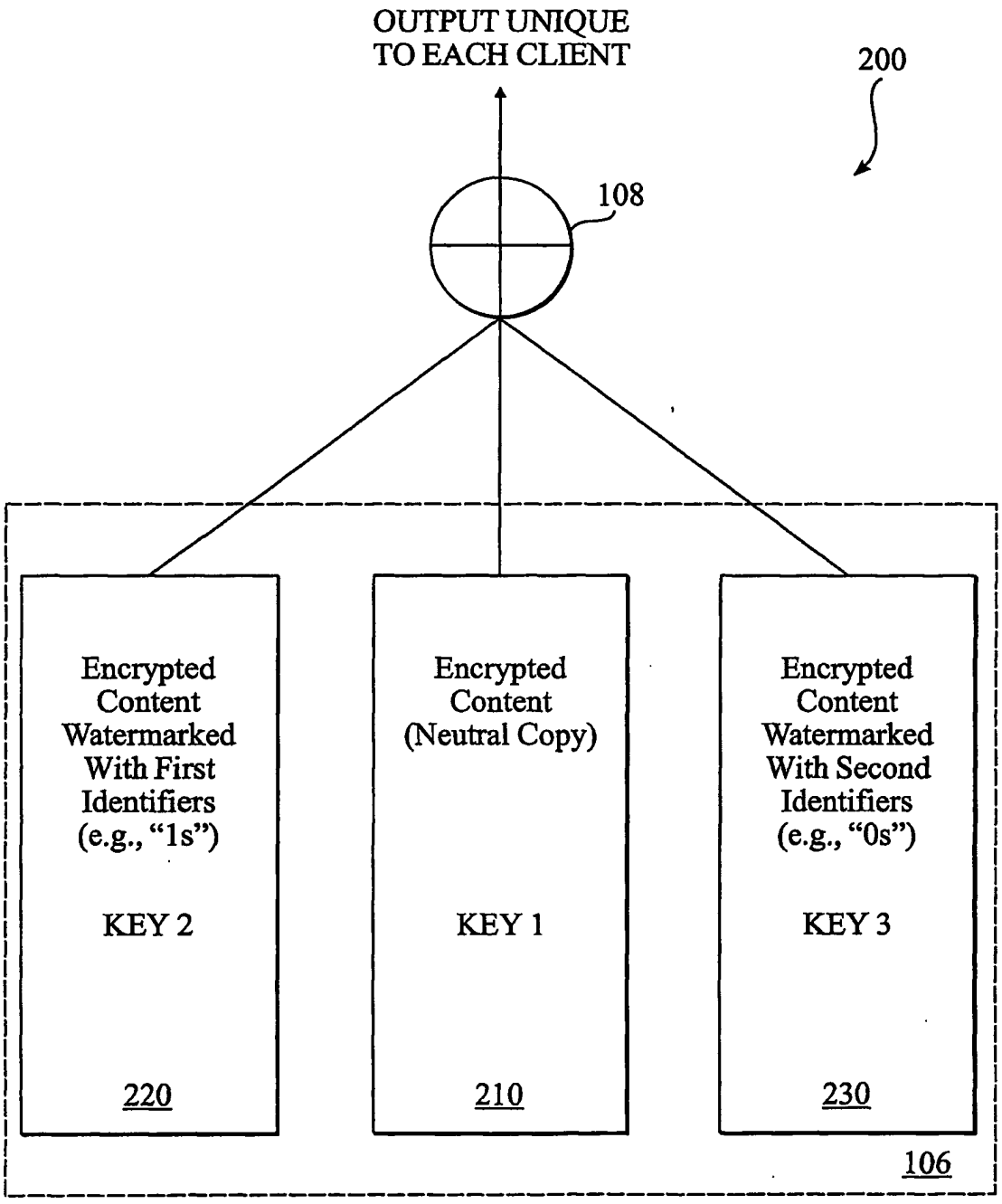

OUTPUT UNIQUE
TO EACH CLIENT
200
108
Encrypted
Content
Watermarked
With First
Identifiers
(e.g., "1s")
KEY 2
220
Encrypted
Content
(Neutral Copy)
KEY 1
210
Encrypted
Content
Watermarked
With Second
Identifiers
(e.g., "0s")
KEY 3
230
106

Fig. 2

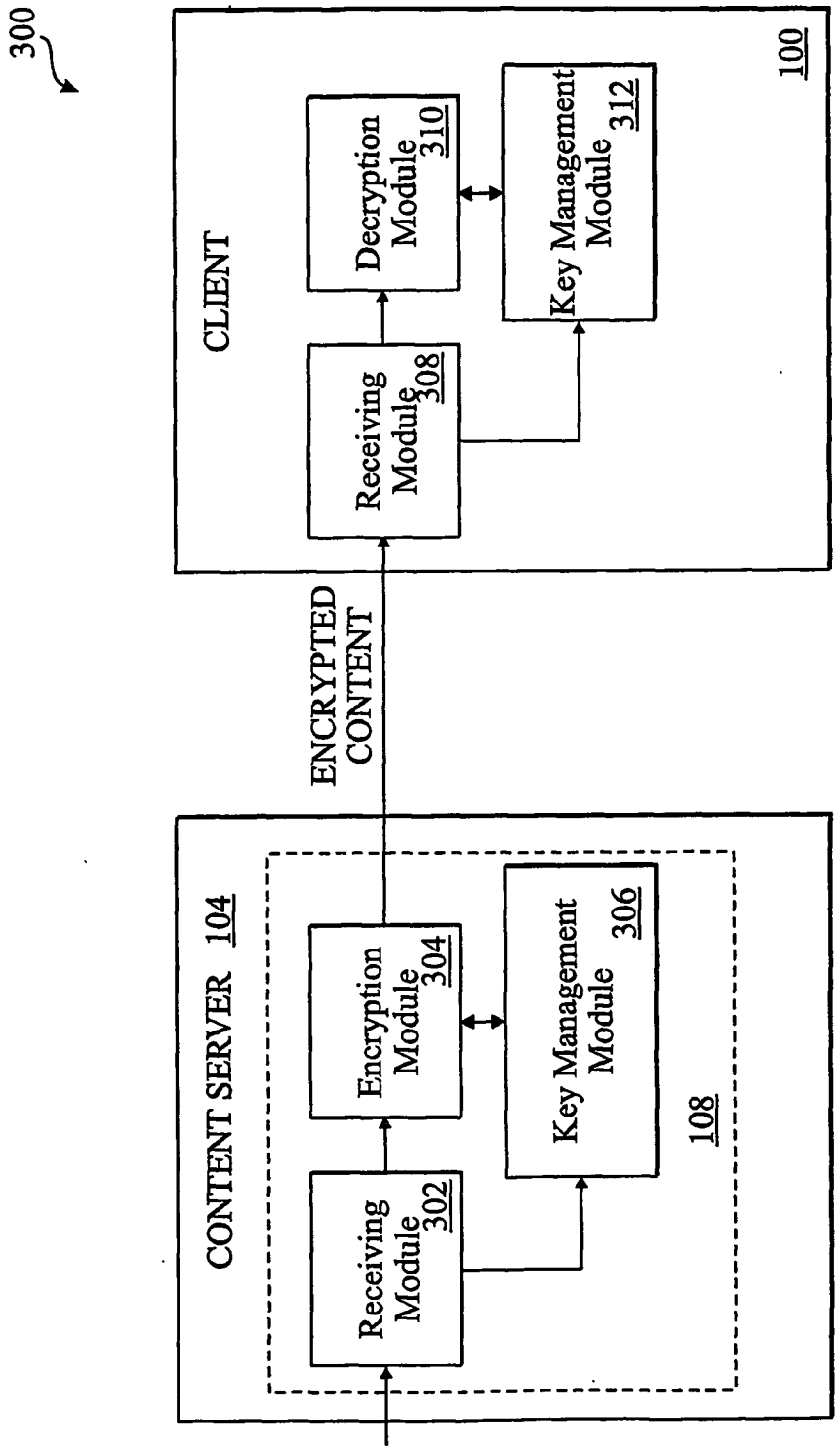

300
CLIENT
100
Decryption Module 310
Key Management Module 312
Receiving Module 308
ENCRYPTED CONTENT
CONTENT SERVER 104
Encryption Module 304
Key Management Module 306
Receiving Module 302
108

Fig. 3

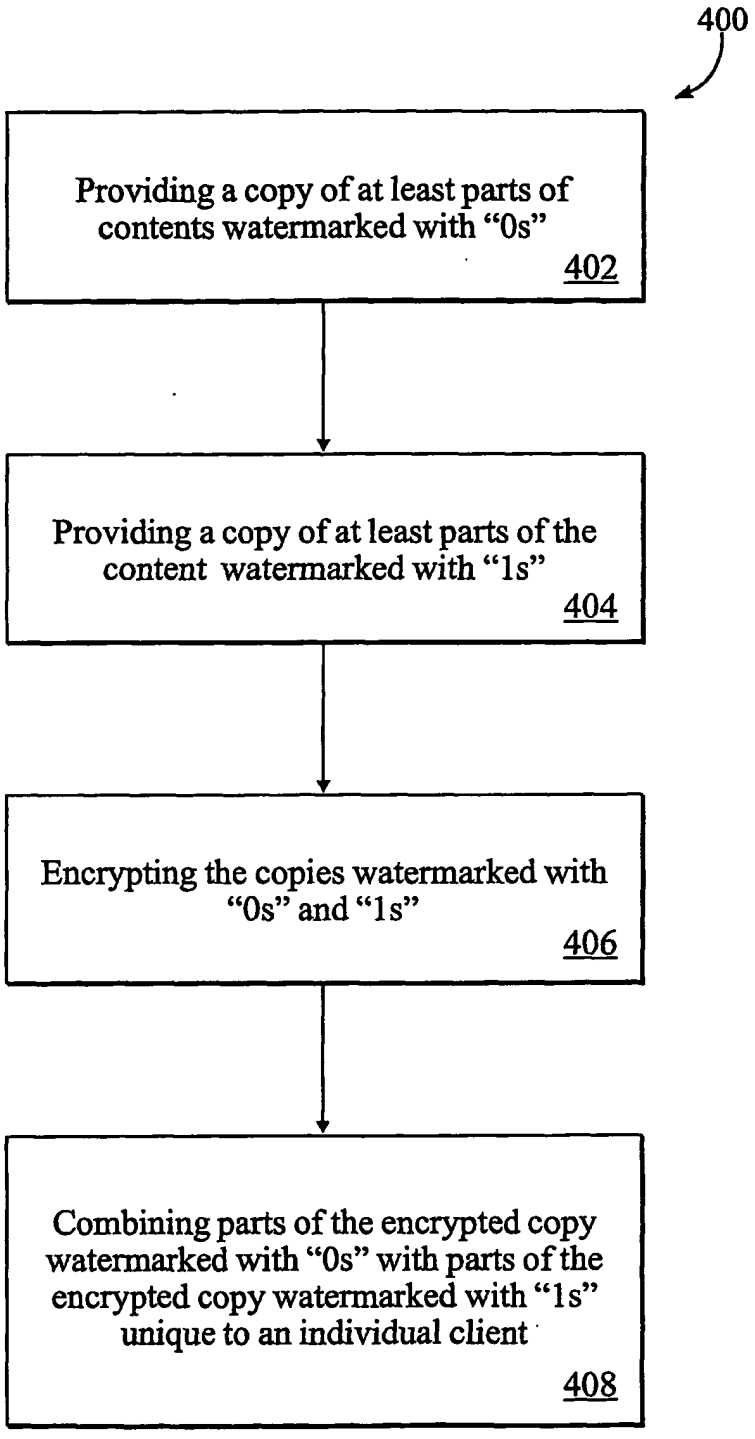

400
Providing a copy of at least parts of contents watermarked with "0s"
402
Providing a copy of at least parts of the content watermarked with "1s"
404
Encrypting the copies watermarked with "0s" and "1s"
406
Combining parts of the encrypted copy watermarked with "0s" with parts of the encrypted copy watermarked with "1s" unique to an individual client
408

Fig. 4A

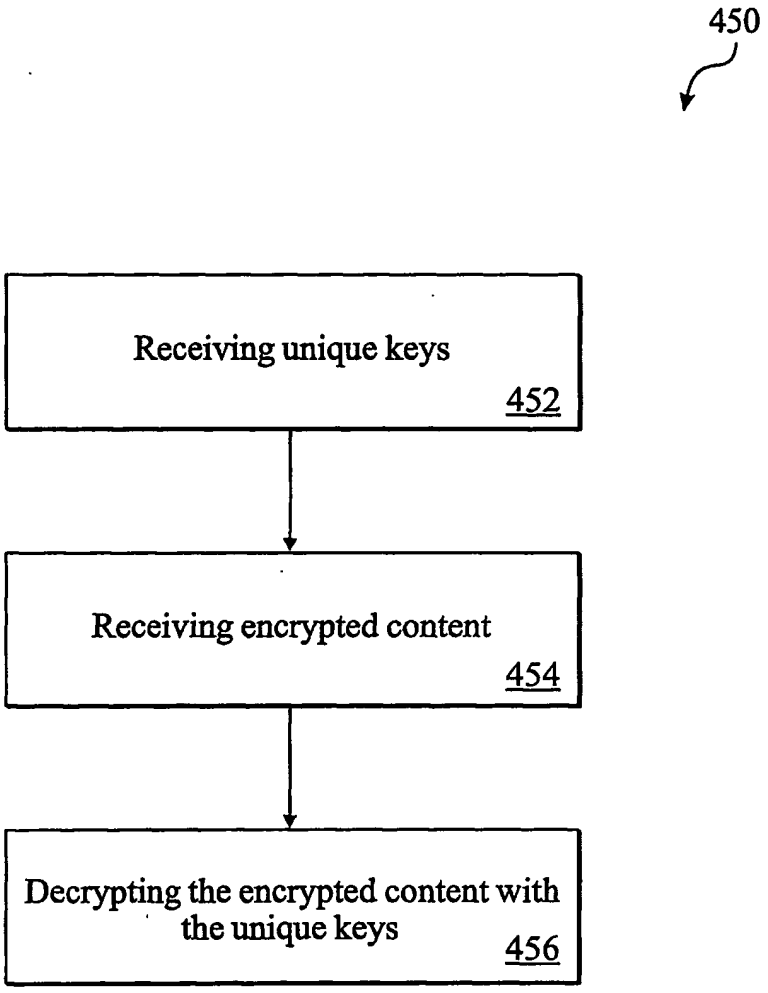

450
Receiving unique keys
452
Receiving encrypted content
454
Decrypting the encrypted content with the unique keys
456

Fig. 4B

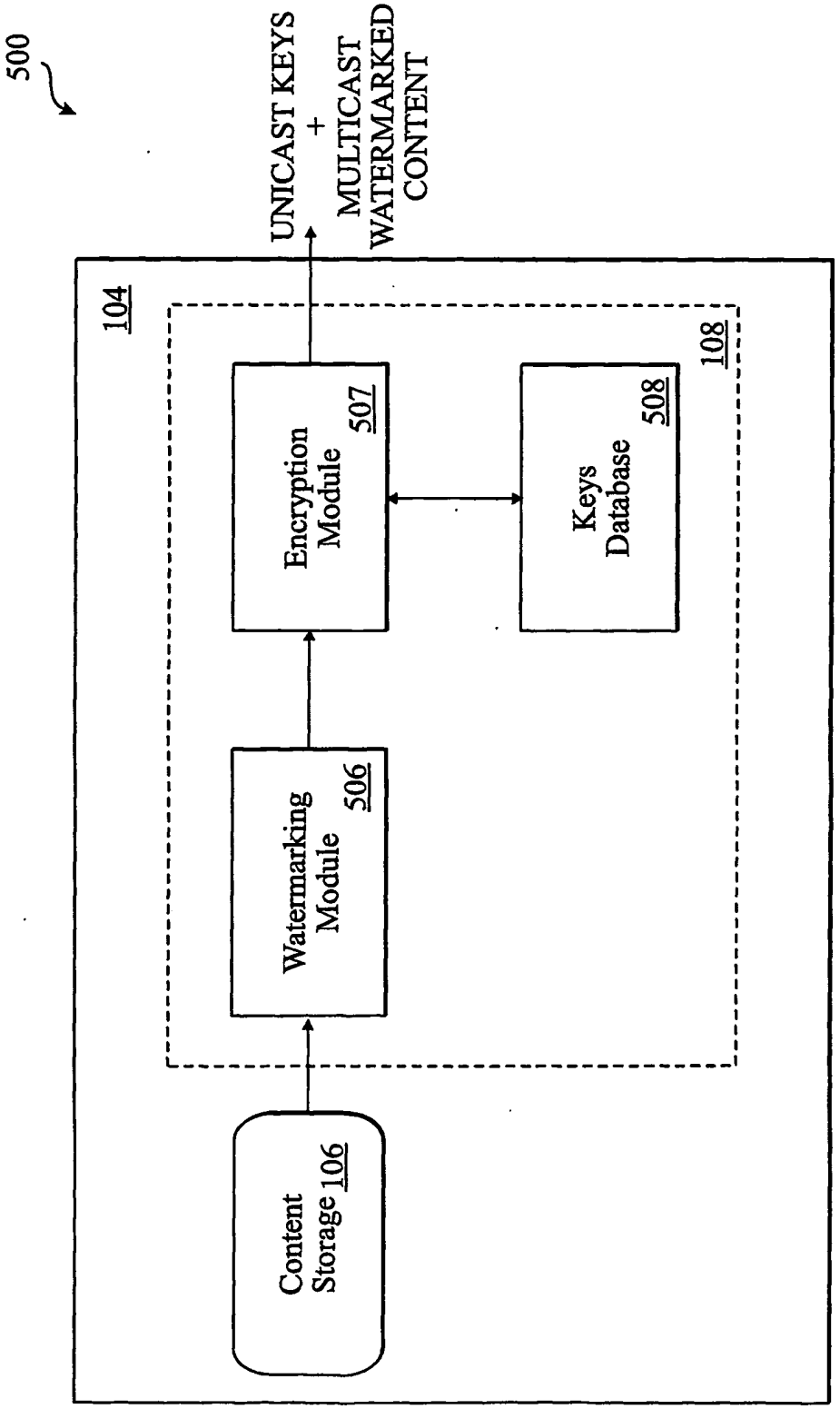

500
UNICAST KEYS
+
MULTICAST
WATERMARKED
CONTENT
104
108
Encryption Module 507
Keys Database 508
Watermarking Module 506
Content Storage 106

Fig. 5

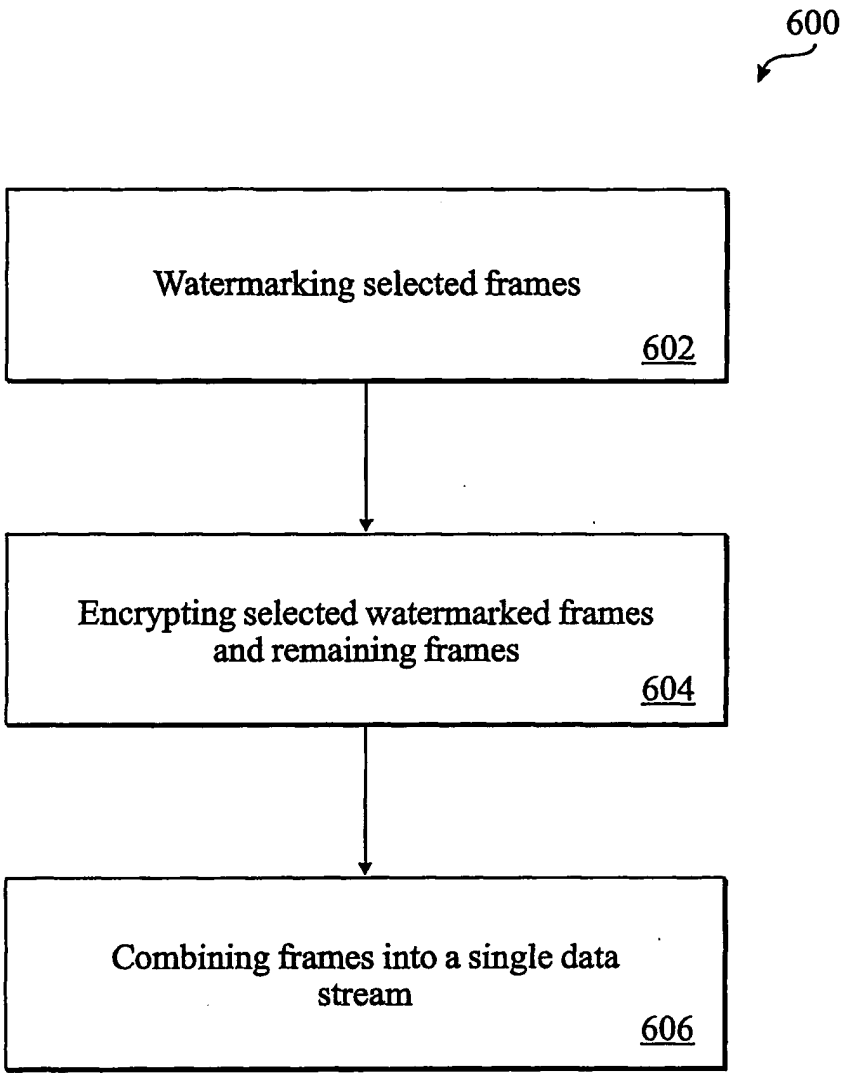

600
Watermarking selected frames
602
Encrypting selected watermarked frames and remaining frames
604
Combining frames into a single data stream
606

Fig. 6A

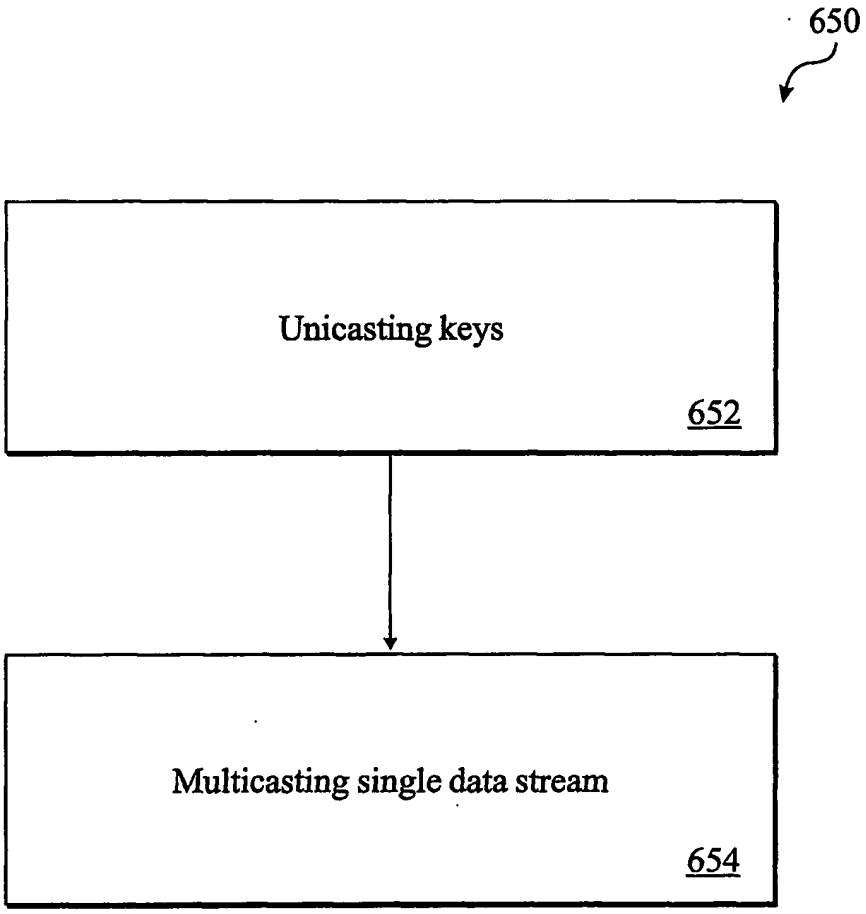

650
Unicasting keys
652
Multicasting single data stream
654

Fig. 6B

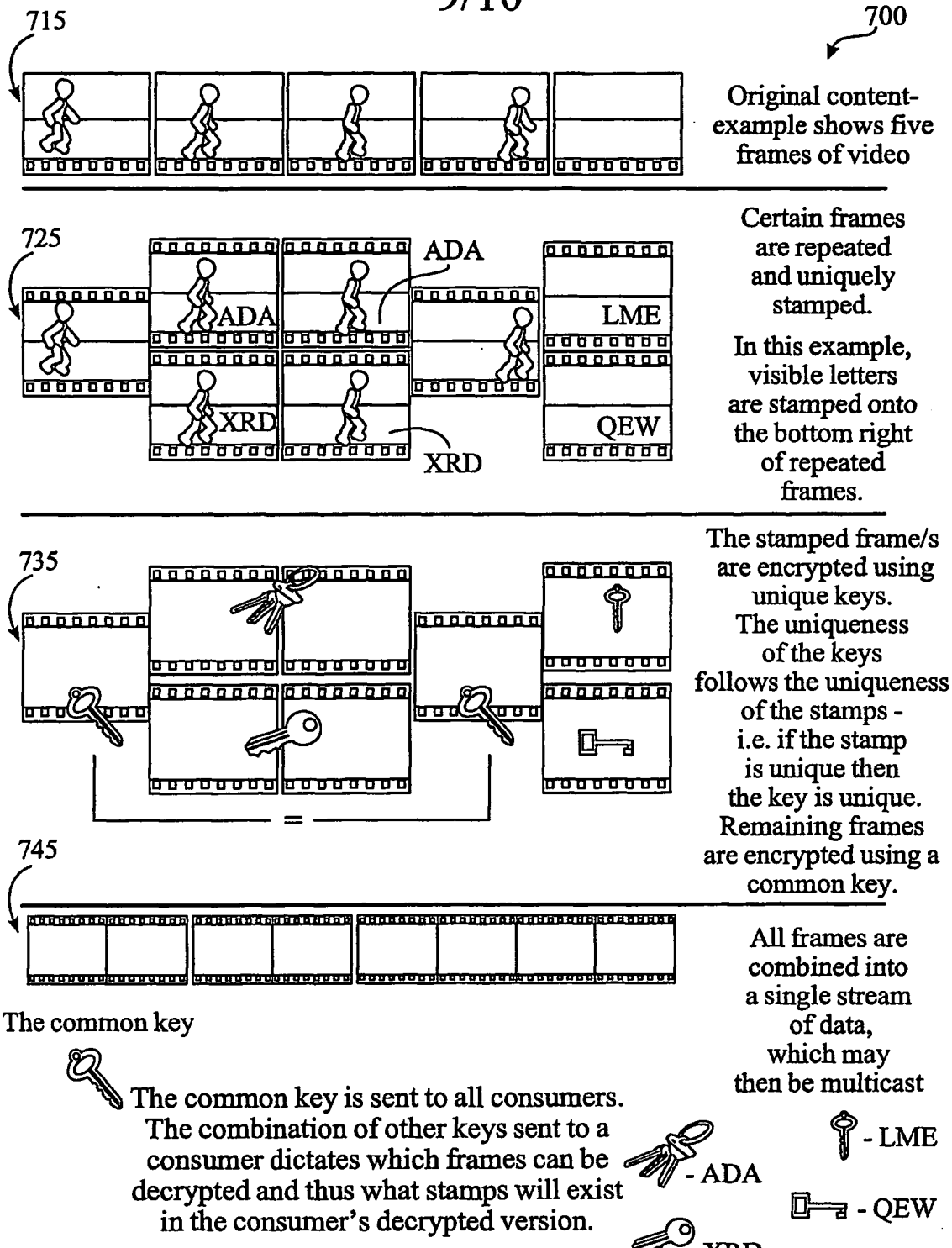

715
700
Original content- example shows five frames of video
725
ADA
ADA
LME
XRD
QEW
XRD
Certain frames are repeated and uniquely stamped.
In this example, visible letters are stamped onto the bottom right of repeated frames.
735
=
The stamped frame/s are encrypted using unique keys. The uniqueness of the keys follows the uniqueness of the stamps - i.e. if the stamp is unique then the key is unique. Remaining frames are encrypted using a common key.
745
All frames are combined into a single stream of data, which may then be multicast
The common key
The common key is sent to all consumers. The combination of other keys sent to a consumer dictates which frames can be decrypted and thus what stamps will exist in the consumer's decrypted version.
- ADA
- LME
- QEW
- XRD

Fig. 7

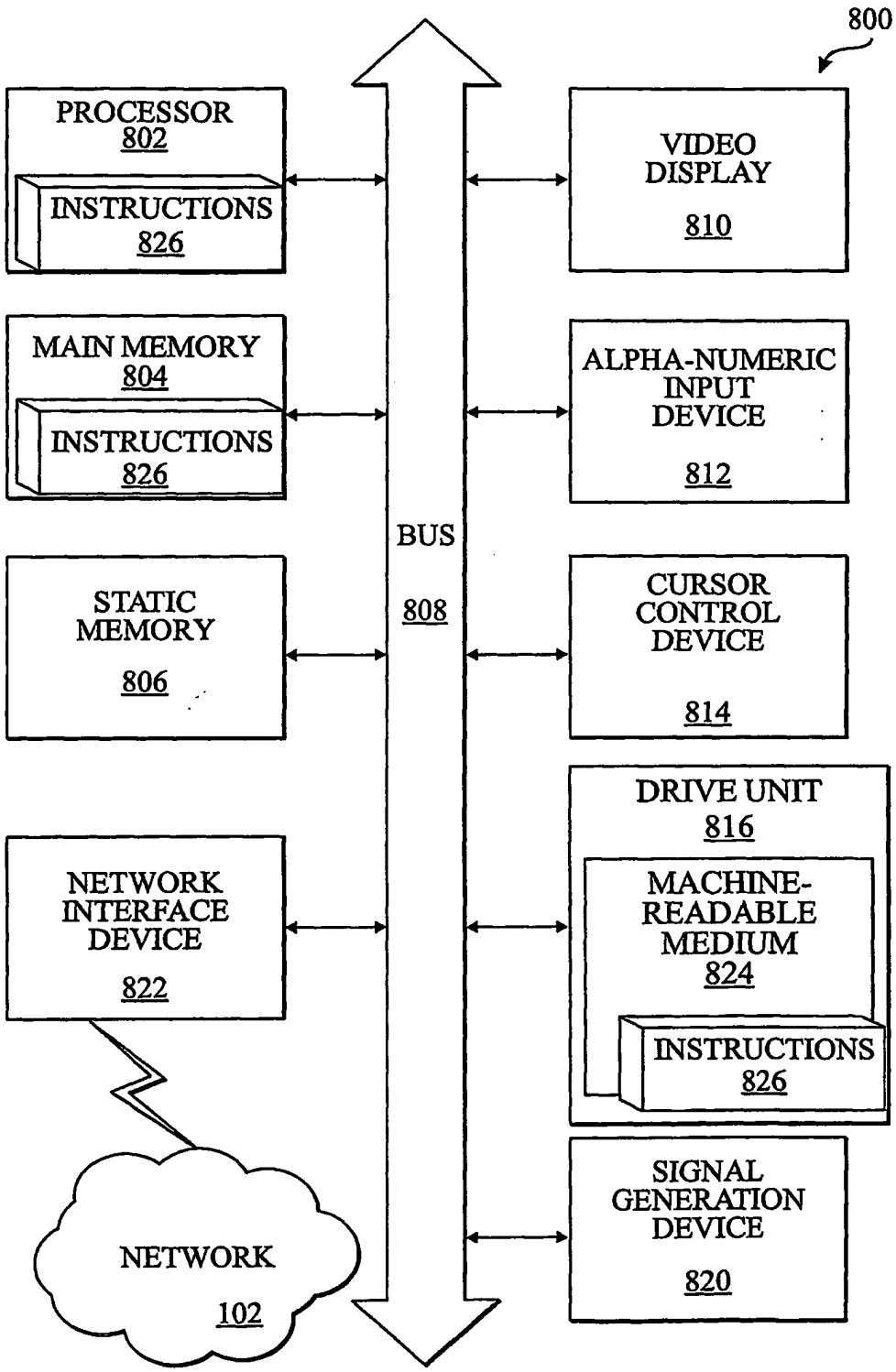

800
PROCESSOR
802
INSTRUCTIONS
826
MAIN MEMORY
804
INSTRUCTIONS
826
STATIC
MEMORY
806
NETWORK
INTERFACE
DEVICE
822
NETWORK
102
BUS
808
VIDEO
DISPLAY
810
ALPHA-NUMERIC
INPUT
DEVICE
812
CURSOR
CONTROL
DEVICE
814
DRIVE UNIT
816
MACHINE-
READABLE
MEDIUM
824
INSTRUCTIONS
826
SIGNAL
GENERATION
DEVICE
820

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/07206

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04L 9/00; H04N 7/167;
US CL :713/176; 380/28,54,200,201; 382/100,232
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/176; 380/28,54,200,201; 382/100,232

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,982,891 A (GINTER et al.) 09 November 1999, col.259, lines 15-36, col.26, lines 5-39.	1-60
Y	US 5,991,426 A (COX et al) 23 November 1999, col.3, lines 20-38, col.11, lines 1-5	1-60
A	US 5,687,236 A (MOSKOWITZ et al) 11 November 1997, col.14, lines 27-64, col.41, lines 62-67, col.42, lines 1-8	1-60

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 27 APRIL 2001	Date of mailing of the international search report 05 JUN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRON James R. Matthews Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet) (July 1998)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/07206

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

STN, EAST
search terms: watermark, encrypt,cipher,encipher,encode,key,finger print,combine,add,multicast,image,picture,video,internet,download,code,password